Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Form PCT/IPEA/416
2003P08757WO		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2004/051153	17.06.2004	18.06.2003
International Patent Classification (IPC) or national classification and IPC		
Applicant		
SIEMENS AKTIENGESELLSCHAFT		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 11 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☒ *(sent to the applicant and to the International Bureau)* a total of 7 sheets, as follows:
      ☒ sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☒ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s))

      _____, containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☒	Box No. VII	Certain defects in the international application
☒	Box No. VIII	Certain observations on the international application

Date of submission of the demand	Date of completion of this report
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/EP2004/051153

Box No. I Basis of the report

1. With regard to the language, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This report is based on translations from the original language into the following language _____, which is the language of a translation furnished for the purposes of:

☐ international search (Rule 12.3 and 23.1(b))

☐ publication of the international application (Rule 12.4)

☐ international preliminary examination (Rule 55.2 and/or 55.3)

2. With regard to the elements of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

☐ the international application as originally filed/furnished

☒ the description:

pages 1-24 as originally filed/furnished

pages* 25,26 received by this Authority on 15.04.2005 with letter of 12.04.2005

pages* _____ received by this Authority on _____

☒ the claims:

nos. _____ as originally filed/furnished

nos.* _____ as amended (together with any statement) under Article 19

nos.* 1-14 received by this Authority on 10.08.2005 with letter of 04.08.2005

nos.* _____ received by this Authority on _____

☒ the drawings:

sheets 1/7-7/7 as originally filed/furnished

sheets* _____ received by this Authority on _____

sheets* _____ received by this Authority on _____

☐ a sequence listing and/or any related table(s) – see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, nos. _____

☐ the drawings, sheets/figs _____

☐ the sequence listing *(specify)*: _____

☐ any table(s) related to sequence listing *(specify)*: _____

4. ☒ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

☐ the description, pages _____

☒ the claims, nos. 1,12-14

☐ the drawings, sheets/figs _____

☐ the sequence listing *(specify)*: _____

☐ any table(s) related to sequence listing *(specify)*: _____

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/EP2004/051153

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-14	YES
	Claims		NO
Inventive step (IS)	Claims	11	YES
	Claims	1-10, 12-14	NO
Industrial applicability (IA)	Claims	1-14	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

1. This report makes reference to the following documents:

D1: "Internet Key Exchange (IKEv2) Protocol", XP015002237

D2: "Internet X.509 Public Key Infrastructure", XP015002989

2. The subject matter of the originally submitted claim 1 does not involve an inventive step (PCT Article 33(3)).

2.1 Apart from the problem of lack of clarity (see Box VIII), D1 discloses most of the features of claim 1 (the references in parentheses are to that document):

process ("IKE", chapter 1.2) for forming an encrypted message (page 8, lines 27-31) which contains communication configuration data ("CP payload", page 31, lines 14-16), in which

- an internet-based authentication process is carried out using at least one service of a unit

of a security layer between a first communication unit and a second communication unit ("IKE supports...EAP", page 28, line 29 - page 29, line 1),

- and the communication configuration data are encrypted by the first communication unit using at least one cryptographic key ("SK_e", page 8, lines 27-29), thus forming the encrypted message ("SK{...}", page 8, lines 27-29).

2.2 The subject matter of claim 1 differs from the disclosure of D1 in that at least one pair of cryptographic keys is formed by the authentication process and in that encryption is carried out using at least one cryptographic key of the pair of cryptographic keys.

2.3 The objective technical problem is that of reinforcing cryptographic protection of the encrypted data.

2.4 The formation of a pair of cryptographic keys by an authentication process and the use of one of the keys of this pair of keys for encryption is a conventional measure, known for example from D2 (paragraphs 4.4.2-4.4.3). Applying this measure would be suggested by the reference to PKIX in D1 (page 82, lines 1-3), for example.

3. The subject matter of the originally submitted independent claims 12-14 does not involve an

inventive step (PCT Article 33(3)).

3.1 Most of the features of the process claim 12 correspond to the features of the non-inventive process claim 1. In addition, claim 12 also mentions that data are recovered by decryption, which is also known from D1 (page 26, lines 21-26). The observations on claim 1 thus also apply to claim 12.

3.2 The features of the independent device claim 13 correspond entirely to the features of the non-inventive process claim 1.

3.3 The features of the independent device claim 14 correspond entirely to the features of the non-inventive process claim 12.

4. The additional features of dependent claims 2-10 do not make an inventive contribution to the independent claims because these features are either known from the above-mentioned prior art (extensible authentication protocol, dynamic terminal configuration) or are conventional measures (network elements, mobile radio network and terminals).

5. Assuming that the term "internet-based" in the original claim 1 had been unambiguously defined according to the complete wording of claim 4, and taking into account the applicant's arguments, dependent claim 11, which refers back to the

original claim 1, appears to contain a novel and inventive subject matter.

5.1 D1 discloses most features of claim 11; see also paragraph 2.1.

5.2 The objective technical problems are that of transmitting in a secure manner IP configuration data to a terminal at a point in time when no IP connection can be established yet, and that of reinforcing cryptographic protection of encrypted data.

5.3 Claim 11 solves these problems in that communication configuration data having the protocol format of a dynamic host configuration protocol are transmitted from the first communication unit to the second communication unit by means of electronic messages using the extensible authentication protocol, and in that a pair of cryptographic keys is formed and encryption is carried out using one of the cryptographic keys of the pair of keys.

5.4 The closest prior art neither discloses nor suggests the solution proposed. In D1, configuration data are exchanged using only an IP protocol. DHCP configuration data for allocating IP addresses are not mentioned, nor is there any suggestion of non-IP, protected data transmission. D2 relates only to the use of certificates in the field of a key infrastructure for reinforced

Box No. V — Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

transmission security, but fails to mention DHCP configuration data and encryption without an IP protocol. The remaining international search report citations are either limited to the secure transmission of configuration data over IP, non-secured transmission of DHCP messages, or secured transmission of authentication data without DHCP messages at the security layer.

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/EP2004/051153

Box No. VII **Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:

1. The independent claims are not drafted in the two-part form recommended by PCT Rule 6.3(b).

2. The features of the claims are not followed by reference signs (PCT Rule 6.2(b)).

Box No. VIII **Certain observations on the international application**

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. In claim 1, the term "internet-based" is ambiguous, when used in association with "authentication processes", since it can be understood as authentication via internet (IP) protocol, authentication by special internet IETF standard protocols or authentication over the internet network (PCT Article 6).

2. The expression "unit of a security layer" is not defined in claim 1 and could be understood, for example, as a component of the abstract OSI layer model. The technical feature for which protection is actually sought is therefore unclear (PCT Article 6).

3. The observations in points 1 and 2 above also apply to the other independent claims, claims 12-14.

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

BOX I

1. The amended independent claims 1, 12, 13 and 14 submitted by the applicant introduce substantive matter which goes beyond the original disclosure in the international application as filed, thereby contravening PCT Article 34(2)(b).

1.1 Th feature that the internet-based authentication process transmits messages "based on the internet protocol standard" was added to claim 1.

However, this wording could be construed to mean that the subject matter of claim 1 also includes authentication processes which run at a higher layer over the internet protocol, such as authentication for internet home banking over an application protocol, layer 7.

This is an inadmissible generalisation, since the original application contained only "internet-based authentication processes at layer 3", "extensible authentication protocol", "protected extensible authentication protocol", "extensible authentication protocol tunnelled TLS authentication protocol" and "protocol for carrying authentication for network access" (see page 9, lines 22-33; and page 11, lines 10-20, of the description).

Supplemental Box

1.2 This also applies to independent claims 12-14.

2. For this reason, only the originally submitted independent claims 1, 12, 13 and 14 have been examined, rather than the amended claims.